

AMENDMENT TO RULES COMM. PRINT 118–10
OFFERED BY MR. TORRES OF NEW YORK

Add at the end of subtitle C of title XVIII the following:

1 SEC. 1859. CRITICAL TECHNOLOGY SECURITY CENTERS.

2 (a) CRITICAL TECHNOLOGY SECURITY CENTERS.—
3 Title III of the Homeland Security Act of 2002 (6 U.S.C.
4 181 et seq.) is amended by adding at the end the following
5 new section:

6 “SEC. 324. CRITICAL TECHNOLOGY SECURITY CENTERS.

7 “(a) ESTABLISHMENT.—Not later than 180 days
8 after the date of the enactment of this section, the Sec-
9 retary, acting through the Under Secretary for Science
10 and Technology, and in coordination with the Director,
11 shall award grants, contracts, or cooperative agreements
12 to covered entities for the establishment of not fewer than
13 two cybersecurity-focused Critical Technology Security
14 Centers (in this section referred to as ‘Centers’) to evalu-
15 ate and test the security of critical technology.

16 “(b) EVALUATION AND TESTING.—In carrying out
17 the evaluation and testing of the security of critical tech-
18 nology pursuant to subsection (a), the Centers shall ad-
19 dress the following technologies:

1 “(1) The security of information and commu-
2 nications technology that underpins national critical
3 functions related to communications.

4 “(2) The security of networked industrial equip-
5 ment, such as connected programmable data logic
6 controllers and supervisory control and data acquisi-
7 tion servers.

8 “(3) The security of open source software that
9 underpins national critical functions.

10 “(4) The security of critical software used by
11 the Federal Government.

12 “(c) ADDITION OR TERMINATION OF CENTERS.—

13 “(1) IN GENERAL.—The Under Secretary for
14 Science and Technology may, in coordination with
15 the Director, award or terminate grants, contracts,
16 or cooperative agreements to covered entities for the
17 establishment of additional or termination of exist-
18 ing Centers to evaluate and test the security of crit-
19 ical technologies.

20 “(2) LIMITATION.—The authority provided
21 under paragraph (1) may be exercised except if such
22 exercise would result in the operation at any time of
23 fewer than two Centers.

24 “(d) SELECTION OF CRITICAL TECHNOLOGIES.—

1 “(1) IN GENERAL.—Before awarding a grant,
2 contract, or cooperative agreement to a covered enti-
3 ty to establish a Center, the Under Secretary for
4 Science and Technology shall coordinate with the
5 Director, who shall provide the Under Secretary a
6 list of critical technologies or guidance on such tech-
7 nologies that would be within the remit of any such
8 Center.

9 “(2) EXPANSION AND MODIFICATION.—The
10 Under Secretary for Science and Technology, in co-
11 ordination with the Director, is authorized to expand
12 or modify at any time the list of critical technologies
13 or guidance on technologies referred to in paragraph
14 (1) that is within the remit of a proposed or estab-
15 lished Center.

16 “(e) RESPONSIBILITIES.—In carrying out the evalua-
17 tion and testing of the security of critical technology pur-
18 suant to subsection (a), the Centers shall each have the
19 following responsibilities:

20 “(1) Conducting rigorous security testing to
21 identify vulnerabilities in such technologies.

22 “(2) Utilizing the coordinated vulnerability dis-
23 closure processes established under subsection (g) to
24 report to the developers of such technologies and, as
25 appropriate, to the Director, information relating to

1 vulnerabilities discovered and any information nec-
2 essary to reproduce such vulnerabilities.

3 “(3) Developing new capabilities for improving
4 the security of such technologies, including vulner-
5 ability discovery, management, mitigation, and reme-
6 diation.

7 “(4) Assessing the security of software,
8 firmware, and hardware that underpin national crit-
9 ical functions.

10 “(5) Supporting existing communities of inter-
11 est, including through grant making, in mitigating
12 and remediating vulnerabilities discovered within
13 such technologies.

14 “(6) Sharing findings to inform and support
15 the future work of the Cybersecurity and Infrastruc-
16 ture Security Agency.

17 “(f) RISK BASED EVALUATIONS.—Unless otherwise
18 directed pursuant to guidance issued by the Under Sec-
19 retary for Science and Technology or Director under sub-
20 section (d), to the greatest extent practicable activities
21 carried out pursuant to the responsibilities specified in
22 subsection (e) shall leverage risk-based evaluations to
23 focus on activities that have the greatest effect on the se-
24 curity of the critical technologies within each Center’s
25 remit, such as the following:

1 “(1) Developing capabilities that can detect or
2 eliminate entire classes of vulnerabilities.

3 “(2) Testing for vulnerabilities in the most
4 widely used critical technologies, or vulnerabilities
5 that affect many such critical technologies.

6 “(g) COORDINATED VULNERABILITY DISCLOSURE
7 PROCESSES.—Each Center shall establish, in coordination
8 with the Director, coordinated vulnerability disclosure
9 processes regarding the disclosure of vulnerabilities that—

10 “(1) are adhered to when a vulnerability is dis-
11 covered or disclosed by each such Center, consistent
12 with international standards and coordinated vulner-
13 ability disclosure best practices; and

14 “(2) are published on the website of each such
15 Center.

16 “(h) APPLICATION.—To be eligible for an award of
17 a grant, contract, or cooperative agreement as a Center,
18 a covered entity shall submit to the Secretary an applica-
19 tion at such time, in such manner, and including such in-
20 formation as the Secretary may require.

21 “(i) PUBLIC REPORTING OF VULNERABILITIES.—
22 The Under Secretary for Science and Technology shall en-
23 sure that vulnerabilities discovered by a Center are re-
24 ported to the National Vulnerability Database of the Na-
25 tional Institute of Standards and Technology, as appro-

1 piate and using the coordinated vulnerability disclosure
2 processes established under subsection (g).

3 “(j) ADDITIONAL GUIDANCE.—The Under Secretary
4 for Science and Technology, in coordination with the Di-
5 rector, shall develop, and periodically update, guidance, in-
6 cluding eligibility and any additional requirements, relat-
7 ing to how Centers may award grants to communities of
8 interest pursuant to subsection (e)(5) to mitigate and re-
9 mediate vulnerabilities and take other actions under such
10 subsection and subsection (k).

11 “(k) OPEN SOURCE SOFTWARE SECURITY
12 GRANTS.—

13 “(1) IN GENERAL.—Any Center addressing
14 open source software security may, in consultation
15 with the Under Secretary for Science and Tech-
16 nology and Director, award grants to individual open
17 source software developers and maintainers, non-
18 profit organizations, and other non-Federal entities
19 as determined appropriate by any such Center, to
20 fund improvements in the security of the open
21 source software ecosystem.

22 “(2) IMPROVEMENTS.—A grant awarded under
23 paragraph (1) may include improvements such as
24 the following:

25 “(A) Security audits.

1 “(B) Funding for developers to patch
2 vulnerabilities.

3 “(C) Addressing code, infrastructure, and
4 structural weaknesses, including rewrites of
5 open source software components in memory-
6 safe programming languages.

7 “(D) Research and tools to assess and im-
8 prove the overall security of the open source
9 software ecosystem, such as improved software
10 fault isolation techniques.

11 “(E) Training and other tools to aid open
12 source software developers in the secure devel-
13 opment of open source software, including se-
14 cure coding practices and secure systems archi-
15 tecture.

16 “(3) PRIORITY.—In awarding grants under
17 paragraph (1), a Center shall prioritize, to the great-
18 est extent practicable, the following:

19 “(A) Where applicable, open source soft-
20 ware components identified in guidance from
21 the Director, or if no such guidance is so pro-
22 vided, utilizing the risk-based evaluation de-
23 scribed in subsection (f).

1 “(B) Activities that most promote the
2 long-term security of the open source software
3 ecosystem.

4 “(1) BIENNIAL REPORTS TO UNDER SECRETARY.—
5 Not later than one year after the date of the enactment
6 of this section and every two years thereafter, each Center
7 shall submit to the Under Secretary for Science and Tech-
8 nology, Director, and the appropriate congressional com-
9 mittees a report that includes the following:

10 “(1) A summary of the work performed by such
11 Center.

12 “(2) Information relating to the allocation of
13 Federal funds at such Center.

14 “(3) A list of critical technologies studied by
15 such Center.

16 “(4) A description of each vulnerability that has
17 been publicly disclosed pursuant to subsection (g),
18 including information relating to the corresponding
19 software weakness.

20 “(5) An assessment of the criticality of each
21 such vulnerability.

22 “(6) An overview of the methodologies used by
23 such Center, such as tactics, techniques, and proce-
24 dures.

1 “(7) A description of such Center’s development
2 of capabilities for vulnerability discovery, manage-
3 ment, and mitigation.

4 “(8) A summary of such Center’s support to ex-
5 isting communities of interest, including an account-
6 ing of dispersed grant funds.

7 “(9) For such Center, if applicable, a summary
8 of any grants awarded during the period covered by
9 the report that includes the following:

10 “(A) An identification of the entity to
11 which each such grant was awarded.

12 “(B) The amount of each such grant.

13 “(C) The purpose of each such grant.

14 “(D) The expected impact of each such
15 grant.

16 “(10) The coordinated vulnerability disclosure
17 processes established by such Center.

18 “(m) REPORTS TO CONGRESS.—Upon receiving the
19 reports required under subsection (l), the Under Secretary
20 for Science and Technology shall submit to the appro-
21 priate congressional committees a summary of such re-
22 ports, and, where applicable, an explanation for any devi-
23 ations in the list of critical technologies studied by a Cen-
24 ter from the list of critical technologies or guidance relat-

1 ing to such technologies provided by the Director pursuant
2 to subsection (d).

3 “(n) CONSULTATION WITH RELEVANT AGENCIES.—

4 In carrying out this section, the Under Secretary shall
5 consult with the heads of other Federal agencies con-
6 ducting cybersecurity research, including the following:

7 “(1) The National Institute of Standards and
8 Technology.

9 “(2) The National Science Foundation.

10 “(3) Relevant agencies of the Department of
11 Energy.

12 “(4) Relevant agencies of the Department of
13 Defense.

14 “(o) AUTHORIZATION OF APPROPRIATIONS.—There
15 are authorized to be appropriated to carry out this section
16 the following:

17 “(1) \$42,000,000 for fiscal year 2024.

18 “(2) \$44,000,000 for fiscal year 2025.

19 “(3) \$46,000,000 for fiscal year 2026.

20 “(4) \$49,000,000 for fiscal year 2027.

21 “(5) \$52,000,000 for fiscal year 2028.

22 “(p) DEFINITIONS.—In this section:

23 “(1) APPROPRIATE CONGRESSIONAL COMMIT-
24 TEES.—The term ‘appropriate congressional com-
25 mittees’ means—

1 “(A) the Committee on Homeland Security
2 of the House of Representatives; and

3 “(B) the Committee on Homeland Security
4 and Governmental Affairs of the Senate.

5 “(2) COVERED ENTITY.—The term ‘covered en-
6 tity’ means a university or federally-funded research
7 and development center, including a national labora-
8 tory, or a consortia thereof.

9 “(3) CRITICAL TECHNOLOGY.—The term ‘crit-
10 ical technology’ means technology that underpins
11 one or more national critical functions.

12 “(4) CRITICAL SOFTWARE.—The term ‘critical
13 software’ has the meaning given such term by the
14 National Institute of Standards and Technology pur-
15 suant to Executive Order 14028 or any successor
16 provision.

17 “(5) OPEN SOURCE SOFTWARE.—The term
18 ‘open source software’ means software for which the
19 human-readable source code is made available to the
20 public for use, study, re-use, modification, enhance-
21 ment, and redistribution.

22 “(6) DIRECTOR.—The term ‘Director’ means
23 the Director of the Cybersecurity and Infrastructure
24 Security Agency.”.

1 (b) IDENTIFICATION OF CERTAIN TECHNOLOGY.—
2 Paragraph (1) of section 2202(e) of the Homeland Secu-
3 rity Act of 2002 (6 U.S.C. 652(e)) is amended by adding
4 at the end the following new subparagraph:

5 “(S) To identify the critical technologies
6 (as such term is defined in section 324) or de-
7 velop guidance relating to such technologies
8 within the remits of the Critical Technology Se-
9 curity Centers as described in such section.”.

10 (c) CLERICAL AMENDMENT.—The table of contents
11 in section 1(b) of the Homeland Security Act of 2002 is
12 amended by inserting after the item relating to section
13 323 the following new item:

“Sec. 324. Critical Technology Security Centers.”.

